WE CLAIM:

1. An energy management device for use in an energy management architecture for managing an energy distribution system, said energy management architecture comprising a network, said energy management device comprising:

an energy distribution system interface operative to couple said energy management device with at least a portion of said energy distribution system;

a network interface operative to couple said energy management device with said network for transmitting outbound communications to said network and receiving inbound communications from said network, said inbound communications comprising first energy management data and said outbound communications comprising second energy management data;

a processor coupled with said network interface and said energy distribution system interface, said processor operative to perform at least one energy management function on said at least said portion of said energy distribution network via said energy distribution system interface, said processor further operative to process said first energy management data and generate said second energy management data as a function of said energy management function;

wherein at least one of said inbound communications comprises a secured inbound communications, said network interface further comprising a security module operative to secure said outbound communications and validate said at least one secured inbound communications.

2. The energy management device of Claim 1, wherein said at least one secured inbound communication is at least encrypted, said security module further operative to at least one of:

a. selectively encrypt said outbound communications; and

b. decrypt said at least one secured inbound communication.

3. The energy management device of Claim 2, wherein said security module is capable of encrypting and decrypting using at least one of Secure Multipurpose Internet Mail Extensions ("S/MIME"), Extensible Markup Language ("XML") Encryption, Secure Sockets Layers ("SSL"), and Pretty Good Privacy ("PGP").

4. The energy management device of Claim 2, wherein said security module is capable of selectively encrypting said outbound communication for decryption only by an intended recipient of said outbound communication.

5. The energy management device of Claim 2, wherein said security module is capable of selectively encrypting said outbound communication for transmission over a portion of said network.

6. The energy management device of Claim 2, wherein said at least one secured inbound communication is further at least signed, said security module further operative to at least one of:

a. selectively sign said outbound communications prior to encryption;

b. selectively sign said encrypted outbound communications;

c. authenticate said at least one secured inbound communication prior to decrypting; and

d. authenticate said at least one secured inbound communication after decrypting.

7. The energy management device of Claim 6, wherein said signed encrypted outbound communications comprises at least one of a public key, a Public Key Infrastructure ("PKI") certificate, a message digest and an Extensible Markup Language ("XML") signature.

8. The energy management device of Claim 6, further comprising a memory coupled with said processor and storing a private key, wherein said security module is further operative to retrieve a first public key of a recipient of said outbound communication via said network if not already obtained, said security module is further operative to one of:

a. encrypt said outbound communications based on said first public key and sign said encrypted outbound communications based on said private key; and

b. sign said outbound communications with said private key and encrypt said signed outbound communications with said public key; and

further wherein said security module is further operative to retrieve a second public key of a sender of said inbound communication via said network if not already obtained, said security module being further operative to one of:

c. decrypt said at least one secured inbound communications based on said private key and authenticate said decrypted at least one secured inbound communications based on said second public key; and

d. authenticate said at least one secured inbound communications based on said second public key and decrypt said authenticated at least one secured inbound communications based on said private key.

9. The energy management device of Claim 2, wherein said outbound communications comprises at least one electronic mail message.

10. The energy management device of Claim 1, wherein said at least one secured inbound communication is at least signed, said security module further operative to at least one of:

a. selectively sign said outbound communications; and

b. authenticate said at least one secured inbound communication.

11. The energy management device of Claim 10, wherein said security module is capable of at least one of signing and authenticating using at least one of PGP, S/MIME, XML Signature, and SSL protocols.

12. The energy management device of Claim 10, wherein said second energy management data is arranged as a plurality of data sets, each of said data sets including at least one data element, said security module being further operative to selectively sign each of said plurality of data sets.

13. The energy management device of Claim 10, wherein said second energy management data comprises a plurality of data elements, said security module being further operative to selectively sign each of said plurality of data elements.

14. The energy management device of Claim 10, wherein said security module is further operative to periodically re-authenticate said at least one secured inbound communication after receipt.

15. The energy management device of Claim 10, wherein said outbound communication comprises Extensible Hypertext Markup Language ("XHTML") data, said security module further comprising an XHTML module operative to sign said outbound communication using XML signing.

16. The energy management device of Claim 10, wherein said security module is further operative to exchange certificates with the sender of the at least one secured communication prior to said signing.

17. The energy management device of Claim 1, wherein said at least one secured inbound communication is at least compressed, said security module being further operative to decompress said at least one secured inbound communication after validation thereof.

18. The energy management device of Claim 1, wherein said security module is further operative to compress said outbound communications prior to the securing thereof.

19. The energy management device of Claim 1, wherein said processor is further operative to generate a first portion of said second energy management data prior to generating a second portion of said second energy management data, said network interface being further operative to generate a first portion of said outbound communication including said first portion of said second energy management data prior to generating a second portion of said outbound communication including said second portion of said second energy management

data, and said security module being further operative to secure said first portion of said outbound communication prior to securing said second portion of said outbound communication.

20. The energy management device of Claim 19, wherein said network interface is further operative to transmit said secured first portion of said outbound communication independent of transmitting said secured second portion of said outbound communication.

21. The energy management device of Claim 1, wherein said network interface is further operative to generate and store said outbound communications when said second energy management data is generated and secure and transmit said outbound communications when said energy management device is not performing said at least one energy management function.

22. The energy management device of Claim 1, wherein said secured outbound communications are capable of being received by a first recipient and retransmitted to a subsequent recipient without compromising authentication by said subsequent recipient.

23. The energy management device of Claim 22, wherein said first recipient may alter the format of said outbound communications for retransmission and retransmit said reformatted outbound communications to said subsequent recipient without compromising authentication by said subsequent recipient.

24. The energy management device of Claim 1, further comprising a memory coupled with said processor, said memory storing a key value and program code executed by said processor to implement said at least one energy management function, said stored program code further being associated with said key value, wherein said processor is further operative to validate said stored program code based on said stored key value.

25. A method of communicating by an energy management device, said energy management device for use in an energy management architecture for managing an energy distribution system, said energy management architecture comprising a network, said method comprising:

coupling said energy management device with at least a portion of said energy distribution system;

coupling said energy management device with said network wherein said energy management device is capable of transmitting outbound communications to said network and receiving inbound communications from said network, said inbound communications comprising first energy management data and said outbound communications comprising second energy management data, wherein at least one of said inbound communications comprises a secured inbound communications;

performing at least one energy management function on said at least said portion of said energy distribution network via said energy distribution system interface, processing said first energy management data and generating said second energy management data as a function of said energy management function; and

securing said outbound communications and validating said at least one secured inbound communications.

26. The method of Claim 25, wherein said at least one secured inbound communication is at least encrypted, said method further comprising at least one of:

encrypting, selectively, said outbound communications; and

decrypting said at least one secured inbound communication.

27. The method of Claim 26, wherein said encrypting and decrypting further comprises using at least one of Secure Multipurpose Internet Mail Extensions ("S/MIME"), Extensible Markup Language ("XML") Encryption, Secure Sockets Layers ("SSL"), and Pretty Good Privacy ("PGP").

28. The method of Claim 26, wherein said encrypting further comprises encrypting said outbound communication for decryption only by an intended recipient of said outbound communication.

29. The method of Claim 26, wherein said encrypting further comprises selectively encrypting said outbound communication for transmission over a portion of said network.

30. The method of Claim 26, wherein said at least one secured inbound communication is further at least signed, said method further comprising at least one of:

signing, selectively, said encrypted outbound communications;

signing, selectively, said outbound communications prior to encryption;

authenticating said at least one secured inbound communication prior to said decrypting; and

authenticating said at least one secured inbound communication after decryption.

31. The method of Claim 30, wherein said signed encrypted outbound communications comprises at least one of a public key, a Public Key Infrastructure ("PKI") certificate, a message digest and an Extensible Markup Language ("XML") signature.

32. The method of Claim 30, further comprising at least one of:

retrieving a first public key of a recipient of said outbound communication via said network if not already obtained;

encrypting said outbound communication based on said first public key and signing said encrypted outbound communication based on a stored private key;

signing said outbound communication based on said stored private key and encrypting said signed outbound communication based on said first public key;

retrieving a second public key of a sender of said inbound communication via said network if not already obtained;

decrypting said inbound communication based on said second public key and authenticating said decrypted inbound communication based on said stored private key; and

authenticating said inbound communication based on said stored private key and decrypting said authenticated inbound communication based on said second public key.

33. The method of Claim 36, wherein said outbound communications comprises at least one electronic mail message.

34. The method of Claim 25, wherein said at least one secured inbound communication is at least signed, said method further comprising at least one of:

signing, selectively, said outbound communications; and

authenticating said at least one secured inbound communication.

35. The method of Claim 34, wherein said signing and authenticating further comprise signing and authenticating using at least one of PGP, S/MIME, XML Signature, and SSL protocols.

36. The method of Claim 34,wherein said second energy management data is arranged as a plurality of data sets, each of said data sets including at least one data element, said method further comprising:

signing, selectively, each of said plurality of data sets.

37. The method of Claim 34, wherein said second energy management data comprises a plurality of data elements, said method further comprising:

signing, selectively, each of said plurality of data elements.

38. The method of Claim 34, wherein said outbound communication comprises Extensible Hypertext Markup Language ("XHTML") data, said method further comprising signing said outbound communication using Extensible Markup Language ("XML") signing.

39. The method of Claim 34, further comprising:

re-authenticating, periodically, said at least one secured inbound communication.

40. The method of Claim 34 further comprising:

exchanging certificates with the sender of the at least one secured communication prior to said signing.

41. The method of Claim 25, wherein said at least one secured inbound communication is at least compressed, said method further comprising decompressing said at least one secured inbound communication after validation thereof.

42. The method of Claim 25, said method further comprising compressing said outbound communications prior to the securing thereof.

43. The method of Claim 25, said method further comprising:

generating a first portion of said second energy management data prior to generating a second portion of said second energy management data;

generating a first portion of said outbound communication including said first portion of said second energy management data prior to generating a second portion of said outbound communication including said second portion of said second energy management data; and

securing said first portion of said outbound communication prior to securing said second portion of said outbound communication.

44. The method of Claim 43, said method further comprising transmitting said secured first portion of said outbound communication independent of transmitting said secured second portion of said outbound communication.

45. The method of Claim 25, said method further comprising generating and storing said outbound communications when said second energy management data is generated and securing and transmitting said outbound communications when said

energy management device is not performing said at least one energy management function.

46. The method of Claim 25, wherein said secured outbound communications are capable of being received by a first recipient and retransmitted to a subsequent recipient without compromising authentication by said subsequent recipient.

47. The method of Claim 46, further comprising:

altering the format of said outbound communications by said first recipient for retransmission and retransmitting said reformatted outbound communications to said subsequent recipient without compromising authentication by said subsequent recipient.

48. The method of Claim 25, further comprising

storing a key value;

storing program code associated with said key value and executable to implement said at least one energy management function;

validating, periodically, said stored program code based on said stored key value.

49. An energy management device for use in an energy management architecture for managing an energy distribution system, said energy management architecture comprising a network, said energy management device comprising:

an energy distribution system interface means for coupling said energy management device with at least a portion of said energy distribution system;

a network interface means for coupling said energy management device with said network for transmitting outbound communications to said network and receiving inbound communications from said network, said inbound communications comprising first energy management data and said outbound communications comprising second energy management data;

a processor means, coupled with said network interface and said energy distribution system interface, for performing at least one energy management

function on said at least said portion of said energy distribution network via said energy distribution system interface, processing said first energy management data and generating said second energy management data as a function of said energy management function;

wherein at least one of said inbound communications comprises a secured inbound communications, said network interface means further comprising a security module means for securing said outbound communications and validating said at least one secured inbound communications.